



# Voting in America

Human and Technical Factors Integral  
to Democratic Elections

**Brian Chess**  
[bchess@fortify.com](mailto:bchess@fortify.com)

**Joy Forsythe**  
[jforsythe@fortify.com](mailto:jforsythe@fortify.com)

**Jacob West,**  
[jwest@fortify.com](mailto:jwest@fortify.com)

# Voting in America

## Human and Technical Factors Integral to Democratic Elections

### Abstract

Elections are the core of the democratic process. In order for an election to remain truly democratic, it must uphold four critical properties: privacy, incoercibility, accuracy and verifiability. In this paper we analyze threats against these properties during the three phases of an election (voter registration, casting votes, and tabulating votes), highlight specific ways voting systems have been compromised, summarize the strengths and weaknesses of current voting techniques, and give guidance for voters to ensure their votes are handled properly in upcoming elections. We conclude with a look to the future of voting systems in America and recommendations for how the federal government and state governments can work with voting machine vendors to adopt business software assurance techniques into the systems they create.

## Table of Contents

---

3	<b>Executive Summary</b>
5	<b>Introduction</b>
6	<b>The Election Process</b>
11	<b>Voting Today</b>
16	<b>The Future</b>
18	<b>Conclusion</b>

## Executive Summary

---

For the past several years, much attention has been focused in the United States on security issues associated with e-voting, and whether a cast vote will ultimately in fact be counted at the polls. The concern is at once so important and seemingly straightforward, that it is surprising to many that a solution hasn't emerged over the course of several national elections. However, America's voting system today is a mixture of many voting systems—each with respective benefits and drawbacks. The real focus of secure elections must harmonize secure technologies alongside effective processes that guarantee four properties of voting:

- **Privacy**—voters have the right to keep their ballots secret.
- **Incoercibility**—voters cannot prove the contents of their cast ballots.
- **Accuracy**—the final tally is the sum of all cast ballots.
- **Verifiability**—voters can prove to themselves that their ballots were cast as intended and counted, and anyone can prove that the final tally is accurate.

### Recommendations:

**1. Any widespread improvement to the election process must detail improvements to both the processes and the technologies used to conduct elections.** Of the two, technology poses the most immediate challenge, because it provides the foundation on which election process and execution are built. Whether a technology enables back-end systems, such as tabulating optical scan ballots, or drives a purely electronic voting mechanism, such as DRE, the fact remains that every scalable system designed to protect privacy, incoercibility, accuracy, and verifiability in an election is controlled by software. Therefore, in order to build software systems that uphold these critical properties, election officials, at both the state and federal level, must work with voting machine vendors to ensure security and robustness is built into the software at the core of elections.

**2. Governments and voting machine vendors should learn from the commercial sector and work together to develop capabilities for building security into voting systems.** Specifically, these capabilities should include code review and penetration testing techniques, such as the ones employed in the 2007 California review, designed to prevent the kind of blatant errors that have been found in code responsible for running voting machines. Consistent review would not only catch such errors but would help in establishing code practices that lead to robust systems.

3. Fortify urges government and voters to follow a recommended preferred ranking of widely available voting techniques:

- **Choice 1—Hand-Counted Paper:** The advantages of hand-counted paper ballots are verifiability and accuracy. Voters can verify their selections before placing ballots in a publicly observable ballot box. After all ballots are cast, they are counted openly to provide public verifiability of the final election.
- **Choice 2—Optical Scan:** Optical scan voting shares many of the advantages of hand-counted ballots and is logistically more convenient and scalable. The accuracy of the counting machines is comparable to that of hand counting.
- **Choice 3—Absentee:** Absentee ballots that are optically scanned may be less accurate, because voters do not have the opportunity to correct overvotes before submitting their ballot. Voters retain their ability to verify that they have recorded their vote as they wish, but they lose the ability to ensure their ballot is counted. They must rely on the postal system to deliver their completed ballot and on election officials to include the ballot in the final tally. Finally, there is no way to ensure incoercibility or privacy for absentee voting, as both are entirely in the hands of the voter.
- **Choice 4—Direct Recording Electronic (DRE):** The primary advantages of these machines are privacy and ease-of-use. The flexible user interface allows many voters, even those with disabilities, to cast their ballots privately and without assistance. However, it is impossible to verify the final tally with an independent count, because the cast votes are only recorded electronically.
- **Choice 5—Lever Machine:** The primary advantage of lever machines is their accuracy, which is similar to that of hand-counted and optical scan ballots. However, lever-voting systems are completely unverifiable. Voters cannot verify that their vote was cast as intended, just that a vote has been cast.
- **Choice 6—Punch Card:** This technique has serious problems in both verifiability and accuracy. It was found to be the least accurate vote-casting method in the 2001 VTP report and is responsible for casting doubt on the results of the 2000 presidential election.

## Introduction

---

The 2000 presidential election in the United States, the outcome of which was not decided until the Supreme Court ruled on December 8, 2000's to end the recounts in Florida, served as a wake-up call to the nation. For the first time, many voters realized how their vote could change an election. The narrow margin and questions surrounding accuracy and fairness sparked a series of investigations into the American election system, many of which uncovered fundamental flaws. These findings, combined with overall voter distrust and \$3 billion in funding from the Help America Vote Act (HAVA), led to an overhaul of American voting systems. However, this overhaul served to amplify the problem, and subsequent elections have demonstrated that significant deficiencies remain.<sup>1</sup>

Elections form the core of democratic society and, as such, are of monumental importance in America and around the world. For an election to serve its purpose in a democracy, it must guarantee four properties:

- **Privacy**—voters have the right to keep their ballots secret.
- **Incoercibility**—voters cannot prove the contents of their cast ballots.
- **Accuracy**—the final tally is the sum of all cast ballots.
- **Verifiability**—voters can prove to themselves that their ballots were cast as intended and counted, and anyone can prove that the final tally is accurate.

Violations of any of these properties, particularly in the form of security breaches, can disrupt the outcome of an election or discourage potential voters from participating. This can allow small groups of people to compromise the robustness and fairness of the election. Any failure to guarantee each citizen the right to cast one, and only one, vote in the election violates the fundamental principle of democracy.

This paper considers the overall capacity for national elections in America to guarantee these properties and proposes ways that both those who orchestrate and those who participate in elections can enhance this capacity. This study evaluates both old and new approaches to conducting elections in terms of threats to privacy, incoercibility, accuracy, and verifiability. It considers threats that impact voter registration, casting votes, and transporting and tabulating ballots. This study also gives recommendations for voters to ensure that their votes are counted and for government organizations that conduct elections to improve the likelihood that future elections are sound. Throughout the paper, we use comparisons to similar requirements and solutions in the banking industry to better understand both why elections are more difficult than banking and to point out ways that elections can benefit from standards and technologies used in other industries.

<sup>1</sup> Rubin, Aviel. *Brave New Ballot*. New York: Morgan Road Books, 2006: 251-268.

## The Election Process

---

Elections comprise three phases:

- **Voter Registration**, where would-be voters declare their desire to participate in the election and communicate information necessary for conducting the election.
- **Casting Votes**, where registered voters communicate their choices by casting ballots.
- **Transporting and Tabulating Votes**, where votes are collected, tabulated, and an outcome is decided.

The privacy, incoercibility, accuracy, and verifiability of an election can be compromised in different ways during each election phase. The remainder of this section discusses various factors that impact these critical properties at each phase, compares and contrasts challenges faced during an election with similar concerns from the financial services industry, and gives examples of real-world failures at each phase. We build on the discussion that begins in this section by evaluating the ability of various voting systems to ensure the critical properties discussed here and provides guidance for voters in selecting the voting techniques that best mitigate these risks.

### Voter Registration

The election process begins with voter registration. During this phase, potential voters must submit personal details to state-maintained databases that allow states to verify voter eligibility. These state-maintained databases store names, addresses, and other personally identifiable information, such as Social Security numbers. States must update their voter databases to reflect new registrations and changes in voters' status that could impact their eligibility, such as death, change of residence, and criminal convictions. To prevent voter registration fraud and ensure the democracy of elections, the Help America Vote Act (HAVA) of 2002 mandates that each state store this information in an electronic form, make it available to all election officials, and connect it to other state-agency databases.<sup>2</sup>

After the requirement that voter rolls be maintained accurately, the biggest concern during voter registration is privacy. Not only could a violation of voter privacy compromise votes during an election, but the voter registration system introduces other risks independent from the election, such as identity theft. Similarly, privacy is one of the biggest concerns in banking transactions. Just as with voter registration, financial institutions must keep records of their users in order to identify them and verify their eligibility to perform transactions, such as accessing funds. Banks typically collect information such as names, addresses, and Social Security numbers along with other personal details about their customers. Furthermore, because of its potential financial value, banking information, such as credit card and account numbers, also represent information that banks must keep private.

<sup>2</sup> Help America Vote Act. 29 Oct 2002 <http://www.fec.gov/hava/hava.htm>.

Motivating the importance placed on privacy in the banking sector are an increasing number of public breaches that have compromised the personal information of hundreds of millions of users. In August of 2008, the Bank of New York Mellon admitted that a data breach had exposed the personal data of 12.5 million customers, including Social Security Numbers.<sup>3</sup> Earlier, the credit card processing firm CardSystems became synonymous with data loss after revealing in 2005 that attackers had compromised credit card information belonging to more than 40 million customers.<sup>4</sup>

Due to a large number of highly publicized exploits like these, the public has become acutely aware that financial institutions are at the frontline in the war to protect their private information. The same attention is not being paid to voter registration data loss, although known breaches have already occurred. In 2006, the state of Ohio revealed that the Social Security numbers of 7.7 million voters were compromised when they were accidentally distributed on CDs given to political campaigns.<sup>5</sup> In 2007, 75,000 voter registration cards in Georgia, complete with Social Security numbers, were found in an Atlanta college's construction trash.<sup>6</sup> Most recently, Pennsylvania was forced to take down an online voter registration site in March of 2008 when it discovered that an authentication error permitted arbitrary users to view details of all past registrants (*InfoWeek*).

## Casting Votes

The process of casting votes is the most discussed area of election security. During this phase, voters must communicate their votes to the government, either by visiting a polling location or through absentee voting. Apart from the final outcome, voters perceive this as the most important phase of the election, because it involves the greatest level of active participation.

All four key properties, privacy, incoercibility, accuracy, and verifiability come to play in this phase of the election. Voters must be able to keep their votes private while casting them, be free from coercion while at the same time being able to verify to themselves that their votes are properly recorded, and finally have assurance that their votes will be included in an accurate measure of the outcome of the election. In this context, concerns around privacy primarily focus on the privacy of the vote being cast, rather than on details about the voter. Perhaps the most difficult challenge at this phase is the inherent tension between incoercibility and verifiability. Voters must be able to verify that their votes were cast as intended, but must not be able to demonstrate their choices to a thirdparty for risk that their vote could be coerced. Accuracy, which is primarily in the domain of transporting and tabulating votes rather than casting them, can also be compromised during this phase if votes are recorded incorrectly or incompletely.

<sup>3</sup> "Bank of NY Mellon data breach now affects 12.5 mln." Reuters 28 Aug 2008  
<http://www.reuters.com/article/marketsNews/idUSWNAB863220080828>.

<sup>4</sup> Evers, Joris. "Details emerge on credit card breach." CNet News 20 June 2005  
[http://news.cnet.com/Details-emerge-on-credit-card-breach/2100-7349\\_3-5754661.html](http://news.cnet.com/Details-emerge-on-credit-card-breach/2100-7349_3-5754661.html).

<sup>5</sup> Weiss, Todd R. "Ohio recalls voter registration CDs; Social Security numbers included." *Computerworld Security* 28 April 2008 [http://www.computerworld.com/action/article.do?articleId=110983&command=viewArticleBasic&intsrc=article\\_pots\\_bot](http://www.computerworld.com/action/article.do?articleId=110983&command=viewArticleBasic&intsrc=article_pots_bot).

<sup>6</sup> "75,000 voter cards dumped in Fulton bin." *Atlanta Journal-Constitution* 13 April 2007: D3.

This phase of an election is most often compared to the banking industry, particularly when contrasting it with the ubiquity, convenience, and effective security of the ATM network. A patent has been filed for using the existing ATM network to cast votes in an election<sup>7</sup> and there have been pilot projects for electronic voting, similar to electronic banking. However, the remainder of this section describes fundamental differences between elections and banking that make these solutions difficult to apply.

In contrast with elections, banking customers demand that their privacy be protected from third parties, but typically not from the bank itself. In fact, banking customers expect that banks will retain a record of transactions, such as deposits and withdrawals, for historical and reporting purposes. In an election, however, voters expect their ballots to be private not only from third parties, but also from the officials conducting the election.

Similarly, customers do not rely on banks to prevent coerced transactions in the same way as in elections. Although the bank might play a roll in preventing coercion by placing cameras at ATM locations or through other security measures, the final responsibility for preventing coercion of financial transactions falls on law enforcement and necessarily involves a combination of proactive and reactive actions. This vulnerability to coercion is unacceptable in an election, where the coerced activity cannot be undone without violating the democracy of the election or repeating the election itself.

Finally, perhaps the most immediate difference between this election phase and the banking industry is related to verifiability. Banks give customers the ability to verify their transactions through paper statements, online banking, and access to bank employees.

Customers are given a receipt after each transaction, which can be used to demonstrate that the transaction occurred. However, none of these options are suitable in an election, because the election must maintain incoercibility.

Failures to ensure privacy, incoercibility, and verifiability during vote casting, which can lead to a loss of accuracy in the overall election, are difficult to identify, because they often occur at a localized level and are lost in scale of the election. One area that often receives a great deal of attention involves accusations of fraud in absentee voting, which clearly suffers from the potential of coercibility. An example of this occurred when former congressman Austin Murphy was convicted in 1999 of voter fraud after forging absentee ballots for nursing home residents.<sup>8</sup>

Poor ballot design can destroy verifiability and accuracy in any form of voting. In Palm Beach County, Florida, the election outcome has been blamed on the “butterfly” ballots, where a single line of circles was used to indicate choices from columns on either side. Many believe that this confusing design is responsible for the Reform Party candidate, Patrick Buchanan, receiving over

<sup>7</sup> Liberman, Barnet. “System and Method for Electronic Voting, Using Existing ATM Network and ATMS Associated Therewith.” WIPO Pub. No. WO/2008/091646 31 July 2008 <http://www.wipo.int/pctdb/en/wo.jsp?WO=2008091646&IA=US2008000894&DISPLAY=STATUS>.

<sup>8</sup> Fund, John. “Democracy Imperiled.” *National Review Online* 13 Sept 2004 <http://www.nationalreview.com/comment/fund200409130633.asp>.

3,000 votes in a heavily democratic district.<sup>9</sup> However, electronic voting machines suffer from ballot design issues as well. During the 2006 election in Florida, close to 13 percent of voters in Sarasota County failed to make a selection in a congressional race, compared to 5 percent in Charlotte County. This might be related to Sarasota choosing to place the congressional race on the same screen as another race, while Charlotte had the race on a separate screen.<sup>10</sup>

## Transporting and Tabulating Ballots

The final phase of an election involves counting votes, which typically requires transporting ballots to central locations where the counting can occur. For example, in Los Angeles County alone, there are over 4 million registered voters spread across 4,383 polling locations that feed into a single tally center.<sup>11</sup> Depending on the media used to record and transport ballots, the process of transferring and tabulating results poses physical challenges, electronic challenges, or both.

The most important property in this phase of the election is verifiability, because verifiability is integral to ensuring the accuracy of the overall election. From the moment voters record their votes, election processes and systems must ensure that votes cannot be tampered with or lost. Any failure to protect ballots, either physical or electronic, can have an impact on the final accuracy of the election and, potentially, its outcome.

American electoral history is full of examples of ballot tampering, most famously, Tammany Hall in New York City and the Daley administration in Chicago. These groups ensured their continued power by stuffing ballot boxes, casting ballots for deceased voters, and other forms of systematic election fraud. Tampering with the ballots after the close of the polls was possible by bribing the election officials responsible for transporting and counting ballots.<sup>12</sup>

Financial institutions rely on armored transport to transfer physical assets and reduce risk by hiring reputable and heavily insured companies to perform this service. Tampering is mostly irrelevant, because there is little motivation for an attacker to alter the assets, whose inherent value is tied to their physical attributes. Transactions involving electronic assets are protected by secure software systems and are often conducted over private networks running on hardware controlled by the financial institution. Even with this level of security, there have been failures. For example, in February of 2008 the compromise of an ATM server resulted in over \$750,000 in losses for Citibank.<sup>13</sup>

<sup>9</sup> Van Natta, Don Jr. "Palm Beach County Had Prior Complaints About Counts." *The New York Times* 17 Nov 2000 <http://query.nytimes.com/gst/fullpage.html?res=9C01EED7123BF934A25752C1A9669C8B63>.

<sup>10</sup>Doig, Matthew. "Analysis suggests undervote caused by ballot design." *The Herald Tribune* 15 Nov 2006 <http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20061115/NEWS/611150751>.

<sup>11</sup>"2008 Statewide Direct Primary Election Media Kit." [http://www.lavote.net/Voter/Media\\_Kit.cfm](http://www.lavote.net/Voter/Media_Kit.cfm).

<sup>12</sup>"History of Voting Technology in the U.S." Online NewsHour 15 Dec 2003 [http://www.pbs.org/newshour/vote2004/primaries/sr\\_technology\\_history.html](http://www.pbs.org/newshour/vote2004/primaries/sr_technology_history.html).

<sup>13</sup>"Citibank debit card fraud highlights ATM vulnerabilities." *ComputerWorld* 7 July 2008 <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9106958>.

Current election procedures attempt to prevent fraud in a variety of ways. Election officials must ensure that every printed ballot is accounted for at all times. If blank ballots are lost, they can be used to corrupt the final tally. At polling locations, votes must be cast and counted in a publicly observable manner. If ballots are counted in the same location as they are cast, it is straightforward for independent monitors to verify the count. If ballots are not counted on site, the election can only be verifiable if ballots are transferred in a manner that prevents tampering. Generally, ballot boxes are sealed in a tamper-evident manner at the polling location and transported to a central election location by a trusted party, such as a law enforcement officer. Once the ballots reach the counting center, the ballot box is examined for tampering before being opened and counted in front of independent monitors. All ballots, even those counted at the polling location, must eventually be transported to a secure location where they can be stored in case they are needed for recounts.

Even with modern election procedures, problems still occur with the transportation and tabulation of physical ballots. At the time of this publication, an August 2008 local election in Palm Beach County is still being disputed. A 60-vote margin of victory triggered a recount, which led officials to discover that roughly 3,500 ballots had disappeared and 176 ballots that were not included in the original count were found. The lost ballots were eventually found in an election warehouse, and election officials claim the ballots were just improperly inventoried and filed, but these discrepancies raise questions about the verifiability of the election.<sup>14</sup> Ominously, this is the same county responsible for the punch card voting controversy that delayed the outcome of the 2000 presidential election.

Transferring electronic media is also problematic. Memory cards are smaller and therefore more easily misplaced than paper ballots, and current technology has been repeatedly shown them to be vulnerable to tampering and corruption.<sup>15</sup> In a September, 2008 election in Washington DC, static electricity and a defective memory card were blamed for discrepancies in a Republican election that drew 3,735 voters. At 9:50pm, 8,246 votes were reported with 1,560 write-ins while, less than 3 hours later, election officials released a total with a corrected number of votes and just 18 write-ins.<sup>16</sup>

<sup>14</sup>“Yet Another Election Drama Swirls in Palm Beach County.” *New York Times* 15 Sept 2008 <http://www.nytimes.com/2008/09/16/us/16florida.html>.

<sup>15</sup>Blaze, Cordero, Engle, Karlof, Sastry, Sherr, Stegers, Yee. “Source Code Review of the Sequoia Voting System.” California Secretary of State’s Top-to-Bottom Review 20 July 2007 [http://www.sos.ca.gov/elections/elections\\_vsr.htm](http://www.sos.ca.gov/elections/elections_vsr.htm).

<sup>16</sup>Stewart, Nikita, and Elissa Silverman. “D.C. Election Glitch Blamed On Equipment.” *Washington Post* 11 Sept. 2008 <http://www.washingtonpost.com/wp-dyn/content/article/2008/09/10/AR2008091000716.html?sid=ST2008091200149>.

## Voting Today

---

Regardless of any current imperfections, elections must continue to take place because they form the foundation of the democratic process. The next presidential election will occur on November 4, 2008, and there are specific choices individual voters can make to increase the likelihood that their vote will be counted as intended. Although options available to voters vary from state-to-state and county-to-county, most voters have access multiple ways to cast their votes. To help voters find out which options are available at their polling location, the Pew Center on the States has published a comprehensive list of voting options by state with links to more detailed information at the local level.<sup>17</sup>

This paper focuses on the voting technology, but people and procedures also have a tremendous sway over the success of elections. Election officials spend months or years working up to a major election. They develop rules and guidelines for every step, from how to distribute ballots to poll locations to how to shut down the polls at night. They hire poll workers and train them, decide how to inform the media and public about results, and determine how and when to audit outcomes. These processes, the human component of the election, can completely change the complexion of the election. However, all of these decisions are built on top of technology—the process cannot be the same for hand-counted paper as for electronic voting.

In order to evaluate how well popular voting technologies uphold the four key properties of an election, we bring together a discussion of their relative strengths and weaknesses with residual vote data from both the 2001 MIT/Caltech Voting Technology Project (VTP) report and subsequent reports using the same methodology.<sup>18</sup> In these reports, researchers estimated accuracy using the number of uncounted, unmarked and overvoted ballots (ballots that contain multiple selections in a contest where only one selection is expected). The table shows our recommended voting techniques in order from most desirable to least desirable and should be used by voters to select the best voting technique available at their polling location. The remainder of this section will discuss the tradeoffs between different voting mechanisms.

<sup>17</sup>Pew Center on the States. "State-by-state Voter Registration System."  
[http://www.pewcenteronthestates.org/template\\_page.aspx?id=42332](http://www.pewcenteronthestates.org/template_page.aspx?id=42332).

<sup>18</sup>CalTech-MIT Voting Technology Project. "Voting—What Is, What Could Be."  
<http://www.votingtechnologyproject.org/2001report.html>.

Table: Preferred order of widely available voting techniques

Number	Voting Technique	Verifiability	Accuracy	Privacy	Incoercibility
1	Hand-Counted Paper: Votes are recorded on paper ballots, which are manually counted by humans.	●	●	○	●
2	Optical Scan: Votes are recorded by hand on paper ballots, but replaces human with computer scanning device for counting.	●	●	○ <sup>1</sup>	●
3	Absentee: Paper ballots are recorded by voters in advance and submitted asynchronously.	○ <sup>2</sup>	●	○	○
4	Direct Recording Electronic (DRE): Votes are directly recorded using an electronic device.	○ <sup>3</sup>	○	●	●
5	Lever Machine: Votes are recorded by pulling specific levers on a mechanical device.	○	●	○	●
6	Punch Card: Votes are recorded by piercing a paper card using a special instrument.	○	○	○	●

<sup>1</sup> Electronic ballot marking devices can allow disabled voters to fill out ballots unassisted.

<sup>2</sup> Absentee balloting has voter verifiability, but lacks overall verifiability.

<sup>3</sup> Only with VVPAT, DRE machines without are not verifiable.

**Choice 1—Hand-Counted Paper:** The advantages of hand-counted paper ballots are verifiability and accuracy. Voters can verify their selections before placing ballots in a publicly observable ballot box. After all ballots are cast, they are counted openly to provide public verifiability of the final election. Hand counting has been shown to be one of the most accurate tabulation methods. For ballots marked by hand, privacy and verifiability are an issue for those without the ability to read or mark their own ballots. This method is most common in rural areas where there is no need for separate polling and counting locations. Transporting the ballots to a separate counting location reduces verifiability, because it is more difficult to detect fraud without preliminary precinct counts.

If this option is available and the counting is done at the polling site, it is the most accurate and verifiable option. Only ten states still use hand-counted ballots in their smaller voting districts: Alaska, Colorado, Idaho, Kansas, Maine, Montana, New Hampshire, Vermont, West Virginia, and Wisconsin.

**Choice 2—Optical Scan:** Optical-scan voting shares many of the advantages of hand-counted ballots and is logistically more convenient and scalable. The accuracy of the counting machines is comparable to that of hand counting. Even better, machines can be placed in all polling locations and detect overvotes before ballots are officially cast. This gives voters a chance to correct and resubmit ballots that would otherwise be rejected. Finally, voters can verify their ballots are correctly recorded and precinct counts can be verified by recounting the original ballots, either with the optical machines again or by hand.

Optical-scan voting, by itself, lacks privacy and verifiability for disabled voters. However, electronic ballot-marking devices provide interfaces that allow these voters to vote independently and verify their selections.

Optical-scan voting is in use in all but 10 states and roughly 55 percent of voters will use optical scan or paper ballots in the 2008 election.<sup>19</sup> This is the most accurate and verifiable option available to most voters.

**Choice 3—Absentee:** Depending on state election law, voters unable or unwilling to travel to polling locations can cast their ballots by mail. Election officials mail ballots to voters who request them, voters return their completed ballots via mail before the election concludes, and the ballots are counted by hand or with optical scan machines.

Absentee voting is more convenient for many voters, because it allows them to avoid traveling to a polling location. It is based on hand-counted or optical scan voting and shares some of the advantages in accuracy and verifiability. However, the remote aspect changes these properties. Absentee ballots that are optically scanned may be less accurate, because voters do not have the opportunity to correct overvotes before submitting their ballot. Voters retain their ability to verify that they have recorded their vote as they wish, but they lose the ability to ensure their ballot is counted. They must rely on the postal system to deliver their completed ballot and on election officials to include the ballot in the final tally. Finally, there is no way to ensure incoercibility or privacy for absentee voting, as both are entirely in the hands of the voter.

If a polling location lacks one of the properly verifiable voting techniques described above, absentee voting is likely the best option. However, 22 states require some form of excuse for casting absentee ballots; refer to the Pew Center for the States Absentee Voting Guide for more information.<sup>20</sup> Absentee voters sacrifice incoercibility, and possibly privacy, for some measure of individual verifiability and accuracy. Absentee voters should be sure to fill out ballots carefully to ensure they will be counted correctly and to mail them early enough to make certain they will arrive on time. If local election rules allow it, dropping off a completed ballot at a polling location will better ensure it is counted properly.

**Choice 4—Direct Recording Electronic (DRE):** DRE machines allow voters to cast ballots through a computer interface. The machines consist of screens that display instructions and ballot options and either a touch screen or button interface for the voter to select his choices. Most of the machines support additional input devices and audio interfaces. The primary advantages of these machines are privacy and ease-of-use. The flexible user interface allows many voters, even those with disabilities, to cast their ballots privately and without assistance. Election officials prefer the machines because they produce instantaneous results and provide more flexibility by allowing multiple ballots and supporting multiple languages.

<sup>19</sup>“Influx of Voters Expected to Test New Technology,” Ian Urbina 21 July 2008 <http://www.nytimes.com/2008/07/21/us/21voting.html>

<sup>20</sup>“Absentee and Early Voting Laws.” Early Voting Information Center at Reed College 21 Feb 2008 <http://www.earlyvoting.net/states/abslaws.php>.

In the past five years, DRE machines have been vilified for their lack of verifiability. Voters have no way of verifying that the machine has recorded their vote faithfully. It is impossible to verify the final tally with an independent count because the cast votes are only recorded electronically.

Starting in 2002, those wishing to add verifiability have called for a voter-verified paper audit trail (VVPAT). After voters make their selections through the standard DRE interface, a receipt detailing their choices is printed behind glass. Voters can then examine the receipt to ensure their choices are recorded faithfully and either accept or reject the ballot. If the ballot is accepted, the receipt will be put into the ballot box. The tally produced by DRE machines can then be verified by counting the paper receipts. This modification hasn't been 100 percent effective—printers jam and run out of ink and the glass that protects receipts from tamper becomes scratched and difficult to see through.<sup>21</sup> The other major problem with VVPAT is a question of whether the electronic count is the official count. Some security experts feel that the receipts should be counted as the official ballot, not just used for auditing. This essentially turns DRE machines into ballot-marking devices.<sup>22</sup>

Accuracy is also an issue for DRE machines. In 2001, the Vote Technology Project (VTP) report found DRE machines to be less accurate than hand-counted, optical scan, and lever voting. Accuracy problems are related to confusing interfaces and other implementation-dependent factors, making verification even more important. Data from the 2004 general election show that the counties that switched to new DRE machines in 2004, presumably with improved interfaces and designs, had significant improvements in accuracy.<sup>23</sup>

At this point, the history of verifiability and accuracy problems has led many voters to distrust DRE machines. While there have been problems with VVPAT, DRE machines equipped with this modification are still more verifiable than absentee ballots, lever voting, and punch-card ballots. Voters who choose this option should check their receipts carefully before confirming their ballots. In areas where VVPAT is not supported, voters should continue to prefer absentee voting and only vote using DRE machines as a last resort before even less desirable techniques.

<sup>21</sup>Thompson, Clive. "Can You Count on Voting Machines?" *The New York Times* 6 Jan 2008 <http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html>.

<sup>22</sup>Mercuri, Rebecca. "Electronic voting and partial audits." CNet News 21 Feb 2008 [http://news.cnet.com/8301-13554\\_3-9876062-33.html](http://news.cnet.com/8301-13554_3-9876062-33.html).

<sup>23</sup>Stewart, Charles III. "Residual Vote in the 2004 Election." *Election Law Journal*, Vol. 5, No. 2: 158-169 [http://www.votingtechnologyproject.org/journals/ELJ-Stewart\\_06.pdf](http://www.votingtechnologyproject.org/journals/ELJ-Stewart_06.pdf).

**Choice 5—Lever Machine:** Voters cast ballots on lever voting machines by pulling a mechanical lever associated with their desired choice. The machines are mechanical devices that maintain internal running tallies for each ballot position. The primary advantage of lever machines is their accuracy, which is similar to that of hand-counted and optical-scan ballots. However, lever-voting systems are completely unverifiable. Voters cannot verify that their vote was cast as intended, just that a vote has been cast. Verification of tallies is not possible because there are no records of the individual ballots. As with paper-based voting systems, visually and physically impaired voters are denied the right to a secret ballot.

Today, this voting technique is only in use in parts of New York and Pennsylvania. Lever machines have a distinct advantage over punch-card ballots because of their accuracy. However, the lack of any ballot records or verifiability makes them an inferior choice to other voting techniques except punch-card voting.

**Choice 6—Punch Card:** Voters cast punch-card ballots using a special device to locate and puncture a point on a paper card that is associated with their desired choice. This technique has serious problems in both verifiability and accuracy. It was found to be the least accurate vote casting method in the 2001 VTP report and is responsible casting doubt on the results of the 2000 presidential election. The system lacks verifiability because voters have difficulty matching up ballot choices with the punch-card device and cannot check their choices without the machine. Ballots are counted by a special scanning device and can be verified by hand count. However, the voting system lacks any true verifiability as handling the ballots can alter their meaning by inadvertently causing additional choices to be marked. Finally, the challenges voters face using punch-card voting cause many voters to sacrifice their privacy in order to receive assistance in casting their ballot.

Today, this voting technique is only used in nine counties in Idaho. Voters in precincts still using these systems should consider absentee voting, which they can sign up for as late as 6 days before the election.<sup>24</sup>

<sup>24</sup>“Accessible Voting Options.” <http://www.idahovotes.gov/Access/access.htm>.

## The Future

---

Any widespread improvement to the election process must detail improvements to both the processes and the technologies used to conduct elections. Of the two, technology poses the most immediate challenge, because it provides the foundation on which election process and execution are built. Whether a technology enables back-end systems, such as tabulating optical scan ballots, or drives a purely electronic voting mechanism, such as DRE, the fact remains that every scalable system designed to protect privacy, incoercibility, accuracy, and verifiability in an election is controlled by software. Therefore, in order to build software systems that uphold these critical properties, election officials, at both the state and federal level, must work with voting machine vendors to ensure security and robustness is built into the software at the core of elections.

In lieu of systematic improvement to the technologies used in elections, there have been calls for an across-the-board return to the most basic form of voting—hand-counted paper ballots. Voters distrust the manufacturers of voting machines and want to cut them out of the process. However, even the Election Defense Alliance, a group that advocates a return to hand-counted ballots, acknowledges that increased staffing and reduced counting speed would be a challenge. For example, their own estimates show that hand-counting ballots for the 4,382 precincts in Los Angeles County would require an additional 52,596 poll workers. The county already has over 25,000 precinct officers and over 30,000 poll workers, but is still chronically short on both.<sup>25</sup> Urban areas account for over 80 percent of the American population and any potential election system must account for elections of this size.<sup>26</sup>

Software systems are necessary to accommodate an increasingly large, urban, and diverse population of voters and to make the election process inherently inclusive. Current approaches, however, have proven inadequate. In 2003, David Dill and Avi Rubin released a study showing critical flaws in leaked source code from Diebold, a leading voting machine manufacturer.<sup>27</sup> In 2007, California Secretary of State Debra Brown conducted a top-to-bottom review of the voting systems used in the state. As a result of this review, California revoked certification for DRE systems from Premier Election Solutions (Diebold under a new name), Hart InterCivic, and Sequoia Voting Systems. All three systems were criticized for the quality of their software in general, not just their implementations of security features.<sup>28</sup>

<sup>25</sup>“2008 Statewide Direct Primary Election Media Kit.” [http://www.lavote.net/Voter/Media\\_Kit.cfm](http://www.lavote.net/Voter/Media_Kit.cfm).

<sup>26</sup>“Population Distribution In 2005.” U.S. Census June 2007 <http://www.census.gov/population/www/pop-profile/profiledynamic.html>.

<sup>27</sup>Rubin, Aviel. *Brave New Ballot*. New York: Morgan Road Books, 2006: 29.

<sup>28</sup>California Secretary of State’s Top-to-Bottom Review 20 July 2007 [http://www.sos.ca.gov/elections/elections\\_vsr.htm](http://www.sos.ca.gov/elections/elections_vsr.htm).

Although the nature of elections introduces unique problems when compared with other areas, such as banking, the fundamental problem of developing software that behaves as intended is ubiquitous throughout the business sector. The need for Business Software Assurance (BSA) is widely acknowledged among commercial organizations. BSA focuses on the concept that organizations must take security into consideration during planning and design, implementation and testing, and deployment and maintenance in order to adequately mitigate the risks introduced by software.

Starting in 2002, Microsoft pioneered capabilities for building security into software by imposing a top-down strategy to address security risk throughout their software development lifecycle. Bill Gates kicked off the initiative with a now-famous 2002 memo titled “Trustworthy Computing” in which he wrote: “So now, when we face a choice between adding features and resolving security issues, we need to choose security.” Microsoft signaled that it really was serious about security when it called a halt to Windows development later in the year and had the entire Windows division (upward of 8,000 engineers) participate in a security push that lasted for more than two months. In an effort to share its successes with others, Microsoft published the details of its internal secure development lifecycle (SDL) in 2006 in a book titled “*The Security Development Lifecycle*” [Howard and Lipner, 2006] and, more recently, has announced plans to develop and share even stronger capabilities in this area.<sup>29</sup>

In the financial services industry, a variety of inroads have been made in mitigating the security risks introduced by software. Most notably, the Payment Card Industry Data Security Standard (PCI DSS), which mandates security best practices for companies that handle credit card information, and the corresponding Qualified Security Assessor (QSA) certification process for individuals who wish to externally verify an organization’s compliance with the standard, are widely recognized as having improved the overall security of consumers’ credit card information.

Looking at recent reports from California, Florida, and Ohio, it is clear that many in the computer security field are interested in evaluating and improving the technology that underpins elections.<sup>30</sup> However, the current standards and auditing system has failed to provide the impetus. The Election Assistance Commission was set up to oversee the Help America Vote Act, but has been undefended and cannot impose standards on the voting machine manufacturers. They established voluntary standards for voting systems, which do cover security, but focus on accuracy and accessibility. Certification of labs to review systems only began in July 2006, and one lab was decertified just five months later for inadequate testing.<sup>31</sup>

<sup>29</sup><http://www.eweek.com/c/a/Security/Microsoft-Beefs-Up-Security-Development-Lifecycle/>

<sup>30</sup>“Project EVEREST.” Ohio Secretary of State 14 Dec 2007 <http://www.sos.state.oh.us/SOS/Text.aspx?page=4512>.

<sup>31</sup>Drew, Christopher. “U.S. Bars Lab From Testing Electronic Voting.” *New York Times* 4 Jan 2007. <http://www.nytimes.com/2007/01/04/washington/04voting.html>.

Governments and voting machine vendors should learn from the commercial sector and work together to develop capabilities for building security into voting systems. Specifically, these capabilities should include code review and penetration testing techniques, such as the ones employed in the 2007 California review, designed to prevent the kind of blatant errors that have been found in code responsible for running voting machines. Consistent review would not only catch such errors but would help in establishing code practices that lead to robust systems.

## Conclusion

---

On November 4, 2008, the responsibility of voters is to cast their ballot in a manner they believe will ensure that it is counted. Election officials are responsible for running their elections in a manner that best accommodates the weaknesses of the voting systems used. The success of our elections also relies on the efforts of election monitors and the press to ensure any problems are detected and publicized.

Just as important, we must not forget about election systems until October 2012. The American voters cannot return to hand-counted paper ballots, so voting software will continue to be integral to the election process. The software that runs our election must be better and more reliable. The voting public and elections officials must insist on better testing and auditing. Voting manufacturers need to adopt development practices standard across the software industry. They must take responsibility for the security of their products by educating their developers and reforming their processes.

This is not software we use to do business or play games; it is not software that protects our bank account or health records. This is software that protects our democracy.



FORTIFY SOFTWARE INC.

MORE INFORMATION IS AVAILABLE AT [WWW.FORTIFY.COM](http://WWW.FORTIFY.COM)

2215 BRIDGEPOINTE PKWY.  
SUITE 400  
SAN MATEO, CALIFORNIA 94404

TEL: (650) 358-5600  
FAX: (650) 358-4600  
EMAIL: [CONTACT@FORTIFY.COM](mailto:CONTACT@FORTIFY.COM)